

Lerneinheit: Digitales Medienrecht

Lernziele:

Die Teilnehmer lernen die wichtigsten rechtlichen Grundlagen im Umgang mit digitalen Medien – vor allem in Bezug auf das Internet – kennen.

Schwerpunkte dieser Lerneinheit sind:

- Besonderheiten des Datenschutzes
- Datensicherheit
- Urheberrecht
- Betriebs- und Geschäftsgeheimnisse
- Am Ende der Lerneinheit sollen die Teilnehmer diese wichtigen rechtlichen Grundlagen im Umgang mit digitalen Medien kennen und in der Praxis anwenden können.

Medien und Materialien:

1 PC mit Internetzugang pro 2 – 3 Teilnehmer
Nutzerprofil bei PeBBLe, www.pebbleonline.de
Arbeitsblatt „BDSG“ (im Anhang der Lerneinheit)

Gesamtdauer: 110 Min.

Einsatz:

Diese Lerneinheit kann eigenständig durchgeführt werden.

Aus Gründen der besseren Lesbarkeit der Unterlage wurde i. d. R. darauf verzichtet, geschlechtsspezifische Unterscheidungen zu treffen. Auch wenn grammatikalisch der Leser männlichen Geschlechts angesprochen wird, so wird damit selbstverständlich die Leserin der Unterlage ebenso angesprochen.

Einführung in die Thematik

Das Internet macht es möglich – Kommunikation mit jedermann im rasanten Tempo. Früher gab es einen Radiosender und viele Empfänger, heute kann praktisch jeder gleichzeitig Sender und Empfänger sein. Neue Möglichkeiten bringen jedoch auch immer neue Verantwortungen mit sich. In dieser Lerneinheit geht es deshalb um Rechte bzw. Gesetze, die im Umgang mit digitalen Medien – vor allem in Bezug auf das Internet – wichtig sind. Sie lernen hier die wichtigsten rechtlichen Grundlagen zu den Themen Datenschutz, Datensicherheit, Urheberrecht, Betriebs- und Geschäftsgeheimnisse kennen.

Während Ihres Praktikums und später in Ihrer Ausbildung werden Sie ggf. mit vielseitigen Daten in Berührung kommen. Mitunter ist es nicht einfach zu entscheiden, ob diese Daten geschützt sind oder ob Sie darüber z. B. mit Freunden oder Kollegen sprechen dürfen. Datenschutz ist nicht nur für Ihren privaten Bereich relevant, sondern vor allem auch ein wichtiger und sensibler Bereich in jedem Unternehmen.

Beginnen Sie hier mit einer allgemeinen Diskussion zu folgenden Fragen:

1. Mit welchen Daten kommen Sie bei der Arbeit in Berührung?

Geschäftsfeld der Deutschen Bahn	Beispiel für Daten
Sicherheitsdienst	Personalien von Personen
Logistik	Getränkeanzahl, Preise, Lieferanten
Service im Bahnhof	Reisende von Daten: Zielort, Zugticket, Fundsachen, Adressen
Service im Zug	Umsatz, evtl. Zielort
Gleisbau	Standort, Art des Schadens
Fahrwegpflege	Standort, Art des (Baum-)Schadens

Weitere Arbeitsfeld-Beispiele	Beispiel für Daten
Versicherungen	Personalien von Personen, Wertgegenstände, Art des Schadens
Gesundheitsbereich	Personalien von Personen, Erkrankungen, ggf. Familienverhältnisse
Kaufmännischer Bereich	Umsatz, ggf. Personalien von Personen
Hausinstallationen (z.B. Elektrik)	Standort, Wohnverhältnisse

2. Was verstehen Sie unter Datenschutz und welche Daten sind schützenswert?

Leiten Sie eine kurze Diskussion! Notieren Sie ggf. die Zurufe der Teilnehmer, welche Daten geschützt werden müssen. Leiten Sie dann zu folgender Aufgabe über:

Das Bundesdatenschutzgesetz

Bei der Bewerbung und im Rahmen eines Arbeitsverhältnisses erhält der Arbeitgeber viele persönliche Daten. Diese Daten braucht er zum Teil, um seinen Pflichten gegenüber der Sozialversicherung und anderen Einrichtungen nachzukommen. Der „gläserne“ Arbeitnehmer also, über den der Arbeitgeber alles erfährt? Nein, grundsätzlich gilt: Der Arbeitgeber darf nur die Daten verarbeiten, die für die Ausgestaltung des Arbeitsverhältnisses erforderlich sind (z. B. Adresse des Arbeitnehmers).

Dieser Grundsatz leitet sich aus dem Bundesdatenschutzgesetz (BDSG) ab. Danach hat jede Person das Recht, selbst über die Preisgabe und Verwendung ihrer persönlichen Daten zu bestimmen. Dieses Recht wird auch „informelles Selbstbestimmungsrecht“ genannt.

Das bedeutet: **Datenschutz = Schutz personenbezogener Daten von Privatleuten vor missbräuchlicher Verwendung und unbefugtem Zugriff.**

Bearbeiten Sie nun das Arbeitsblatt „Bundesdatenschutzgesetz“, welches sich im Anhang

dieser Lerneinheit befindet.

Die Teilnehmer sollen nun das Arbeitsblatt „Bundesdatenschutzgesetz“ bearbeiten. Leisten Sie ggf. Hilfestellung beim Ausfüllen des Lückentextes. Besprechen Sie im Anschluss gemeinsam mit den Teilnehmern die korrekte Lösung.

Besonderheiten im Datenschutz

Um Ihnen den Umgang mit zu schützenden Daten zu erleichtern, erarbeiten Sie nachfolgend, mit welchen Daten Sie besonders achtsam umgehen müssen:

Methode: Standogramm

Notieren Sie auf Steckkarten „A: Daten müssen nicht geschützt werden“, „B: Daten müssen geschützt werden“ und „C: weiß nicht“. Legen Sie im Raum verteilt drei verschiedene Standorte für die Karten fest und hängen Sie diese sichtbar für alle Teilnehmer auf. Bitten Sie die Teilnehmer sich auf einer freien Fläche im Raum zu sammeln. Die Teilnehmer sollen sich - nachdem Sie ein Beispiel vorgelesen haben – einem der Standorte zuordnen. Lassen Sie beispielhaft jeweils einen Teilnehmer seine Entscheidung begründen.

Folgende Standorte werden im Raum festgelegt:

- A. Daten, die nicht geschützt werden müssen
- B. Daten, die geschützt werden müssen
- C. Keine Ahnung, ob diese Daten zu schützen sind

Es werden verschiedene Beispiele genannt. Bitte wählen Sie Ihren Standpunkt und begründen Ihre Entscheidung.

Beispiele:	Lösung:
Private Handynummer eines Mitschülers	B
Gehalt von Bundeskanzlerin Angela Merkel (wurde bereits in Medienberichten veröffentlicht, kann im Internet nachgelesen werden)	A
Geburtsdatum des Kollegen Max Mustermann	B
Eigene Bankverbindung (BLZ und Kontonummer)	B
Familienstand des Vorarbeiters	B
Anzahl der Sitz- und Stehplätze in der Imtech Arena Hamburg (kann im Internet nachgelesen werden)	A
Tagesumsatz des Supermarktes um die Ecke	B
Ein Foto der letzten Betriebsfeier, auf dem Herr Meier mit Frau Kunze tanzt.	B
Sitzverteilung (Parteien) des Deutschen Bundestages (kann im Internet nachgelesen werden)	A
IP-Adresse (eines PC-Anschlusses), wenn darüber auf eine natürliche Person geschlossen werden kann	B
Gewerkschaftszugehörigkeit	B
Jahresumsatz einer Aktiengesellschaft (muss veröffentlicht werden, bzw. kann beim zuständigen Amtsgericht – Handelsregister – nachgelesen werden. Veröffentlichung ist gesetzlich vorgeschrieben)	A
Passwort in Sozialen Netzwerken	B
Anzahl der Bürger/Bewohner eines bestimmten Stadtteils, z. B. Frankfurt-Eschersheim (Statistik)	A

Finden Sie weitere Beispiele oder lassen Sie die Teilnehmer weitere Beispiele nennen. Geben Sie im Anschluss den Teilnehmern ausreichend Zeit, um sich Notizen zu machen.

Welche der genannten Beispiele würden Sie auf Ihrem Profil (z. B. Facebook) veröffentlichen?

Sie haben nun verschiedene zu schützende Daten kennengelernt. Grundsätzlich unterscheiden wir zwischen personenbezogene Daten und betriebsinterne Daten. Notieren Sie jeweils drei Beispiele.

Personenbezogene Daten	Betriebsinterne Daten

Das Grundprinzip im Datenschutz ist nicht der Schutz der Daten, sondern der Menschen. Die korrekte Anwendung der Datenschutzprinzipien gehört auch zur Unternehmenskultur, in der wir mit Respekt, Achtung und Offenheit miteinander umgehen.

Beim korrekten Umgang mit betriebsinternen Daten schützen die Mitarbeiter das Unternehmen. Eine Offenlegung von Geschäfts- und Betriebsgeheimnissen gegenüber unbefugten Dritten oder der Öffentlichkeit kann zu erheblichen Nachteilen und Schäden für den Betrieb führen.

Regen Sie die Teilnehmer zu einer Diskussion zu Nachteilen/Schäden an. Nutzen Sie dafür ggf. folgende Beispiele: z. B. Imageschaden wegen Verhalten im Zug, Foto oder Verknüpfungen auf Facebook, finanzielle Schäden etc.

Merke: Verstöße gegen den Datenschutz sowie die Offenlegung von betriebsinternen Daten können zu disziplinarischen Maßnahmen führen, die sogar eine Kündigung und Schadensersatzforderungen auslösen.

Lassen Sie die Teilnehmer den Selbsttest zum Identitätsdiebstahl „Self assessment ID-theft“ am PC durchführen. Sie finden den Link in der Gruppe „Regeln der Mediennutzung“ auf www.pebbleonline.de.

Weitere Information über den sicheren Umgang mit Daten erhalten Sie in der erwähnten Gruppe „Regeln der Mediennutzung“ auf PeBBLe.

Wie sicher gehen Sie mit Ihren persönlichen Daten um? Jeder muss seinen Beitrag leisten, damit seine Daten nicht in falsche Hände gelangen und dadurch Nachteile entstehen. Worauf achten Sie beim Umgang mit Ihren Daten?

Nennen Sie Maßnahmen, durch die Sie einen Diebstahl Ihrer persönlichen Daten vorbeugen können.

Diskutieren Sie mit den Teilnehmern, wie diese sich vor dem Verlust ihrer Daten schützen können. Sensibilisieren Sie die Teilnehmer zu einem bewussten und sicheren Umgang mit ihren personenbezogenen Daten.

- Handy verschlüsseln, Handy-Rechnung stets genau kontrollieren
- Brieftasche und Ausweisdokumente nur in Innen-, Bauch- oder vorderen Hosentaschen tragen
- beim Einkauf im Internet auf eine sichere Verbindung achten (https)
- Sparsamer Umgang mit persönlichen Daten im Internet bzw. am Telefon
- Dokumente, persönliche Informationen (Rechnungen, Kontoauszüge) nur geschreddert in die Papiertonne werfen
- sorgfältiger Umgang mit der Sozialversicherungsnummer/Identitätsnummer
- u.a.

Datensicherheit/IT-Sicherheit

Weder im privaten noch im beruflichen Alltag sind moderne Informations- und Telekommunikationstechnologien wegzudenken. Die Nutzung von PC, Laptop und Handy ist zur Normalität geworden, das Suchen und Downloaden von Informationen aus dem Internet zur Gewohnheit.

Sind Sie schon einmal mit einem Angriff auf Ihren PC aus dem Internet in Berührung gekommen? Wenn ja, welche Schwierigkeiten mussten Sie meistern bzw. wie konnte das passieren? Notieren Sie auf Flipchart Ihre Erfahrungen stichpunktartig. Die Auswertung erfolgt dann im Plenum.

Diese Aufgabe kann in Gruppen oder einzeln durchgeführt werden.

Mögliche Antworten:

- Viren (Programm mit Schadfunktion; Der Benutzer aktiviert den Virus, z. B. durch Öffnen eines E-Mail-Anhangs. Ist der Virus einmal aktiviert, kann er bestimmte Aktionen wie das Löschen oder Verändern von Dateien auslösen. Sie verbreiten sich selbständig.)
- Phishing (das Ausspionieren von Passwörtern und PINs)
- Trojaner (Schadprogramme; Sie dienen z. B. zum Sammeln persönlicher Daten, Übermitteln von Benutzergewohnheiten, Versenden von Spam-Mails.)
- Würmer (eine Form von Viren, die nicht erst durch den Benutzer aktiviert werden muss; Es genügt, wenn der PC im Netz ist. Sie besitzen eine Verbreitungsfunktion.)

Welchen Beitrag können Sie zur Gewährleistung der IT-Sicherheit leisten?

Sicherer Umgang mit ITK durch folgende Maßnahmen:

- keinen Benutzer-Account weitergeben
- sicheres Passwort (z. B. keinen Namen, keine einfachen Begriffe, keinen privaten Bezug, für dienstliche Zwecke, andere Passwörter verwenden als im privaten Umfeld)
- PC sperren, wenn der Arbeitsplatz verlassen wird
- vertrauliche und personenbezogene Daten dürfen nicht auf externen Speichermedien abgelegt werden
- E-Mails von nicht vertrauenswürdigen Absendern dürfen nicht geöffnet werden.
- keine Kettenmails weiterleiten

Sicherlich haben Sie bei Ihrer Aufzählung auch an sichere Passwörter gedacht. Vermeiden Sie Passwörter, die einen einfachen Begriff enthalten, Namen oder sonstige private Vorlieben enthalten.

Hier finden Sie Beispiele für unsichere Passwörter:

- Teeküche26
- 22Sommerwind
- Beethoven
- chillen

Sichere Passwörter sollen ein Mix aus Buchstaben (klein und groß), Zahlen und Sonderzeichen sein. Hier ein Beispiel:

- 1WimwaAbwismPä! (1Wenn ich morgen wieder am Arbeiten bin werde ich sofort mein Passwort ändern!)

Übrigens: Laut Statistik sind die am häufigsten verwendeten Passwörter folgende:

- Passwort
- Vornamen von Familienmitgliedern/berühmten Persönlichkeiten

Finden Sie weitere sichere Beispiele für Passwörter und notieren Sie diese hier:

Das Internet macht es möglich – Kommunikation mit jedermann im rasanten Tempo. Früher gab es einen Radiosender und viele Empfänger, heute kann praktisch jeder gleichzeitig Sender und Empfänger sein. Unter dem Begriff „Social Media“ werden webbasierte Anwendungen zum Austausch von Meinungen und Erfahrungen zusammengefasst.

Urheberrecht und das Recht am eigenen Wort und Bild

Leiten Sie kurz folgende Diskussion ein: Was verstehen Sie unter „geistigem Eigentum“?

Was verstehen Sie unter „geistigem Eigentum“?

Als **geistiges Eigentum** (engl. *intellectual property*, kurz *IP*) eines Menschen wird all jenes Wissen und Kulturgut bezeichnet, das dieser sich durch geistige Anstrengungen wie Lernen, Forschen, Nachdenken, Lesen oder auch Diskutieren zu eigen gemacht hat. Der Begriff wird außerdem als Jargon für Urheberrechte und gewerbliche Schutzrechte verwendet, kommt in Gesetzen jedoch nicht vor (Quelle: Wikipedia).

Zum Beispiel sind die Schulungsunterlagen geistiges Eigentum von LernenPlus, die Sie hier während des Praktikums ausgehändigt bekommen. Deshalb dürfen diese Unterlagen nicht anderen Personen, wie z. B. Lehrern oder Freunden zur Verfügung gestellt werden.

Wenn Sie Bilder, Grafiken oder Videos in Ihren PowerPoint-Präsentationen, Flyern oder sonstigen Dateien verwenden, müssen Sie darauf achten, dass Sie auch dort keine Urheberrechtsverletzung eingehen. Bei Grafiken, die durch vorhandene lizenzierte Software (z. B. ClipArt von Microsoft Office) zur Verfügung steht, ist eine Verwendung grundsätzlich erlaubt. Bei der Verwendung von Fotos (z.B. aus Bilddatenbanken) ist grundsätzlich der Fotograf mit Vor- und Familiennamen (oder Künstlernamen) als Urheber zu benennen (Ausnahme: die Verwendung des Bilds/der Bilder ist ausdrücklich ohne Nennung des Erstellers erlaubt oder man ist selbst Urheber der Bilder/Grafiken). Die Urheberbenennung erfolgt unmittelbar am Foto. Andernfalls muss bei Angabe des Namens und der Eigenschaft als Fotograf gewährleistet sein, dass ein Foto dem Fotografen eindeutig zugeordnet werden kann.

Dieses Beispiel zeigt die korrekte Urheberrechtsbenennung:



Regeln für das Veröffentlichen selbst erstellter Medien

Durch den digitalen Wandel kann heute jeder Medien selbst produzieren und verbreiten. Damit es dabei nicht zu rechtlichen Problemen kommt, gilt es folgende Regeln zu beachten:

Nutzung fremder Inhalte

Um ein selbst erstelltes Medium (z. B. eine Video) legal veröffentlichen zu können, benötigt man die Nutzungsrechte aller enthaltenen Medien wie Musik, Bild und Text. Selbsterstellte Medien darf man bedenkenlos nutzen, es ist aber oft unklar, unter welchen Bedingungen man fremde Inhalte benutzen darf. Creative-Commons(CC)-Lizenzen haben den Sinn, die Frage nach den Nutzungsbedingungen einfach und eindeutig zu regeln. Jeder Urheber kann mit Hilfe dieser vorgefertigten Lizenzverträge festlegen, was andere mit seinem Werk tun dürfen und was nicht. Deswegen empfehlen wir für die Nutzung fremder Medien ausschließlich solche, die unter der (passenden) CC-Lizenz veröffentlicht wurden.

Bearbeiten Sie folgende Aufgaben:

Erstellen sie eine offene oder geschlossene Gruppe auf www.pebbleonline.de (z. B. mit dem Namen der Klasse) und laden sie die Teilnehmer hierzu ein. Offene Gruppen lassen sich über die Suchfunktion der Seite finden und jeder kann ihnen beitreten. Geschlossenen Gruppen kann man nur durch einen Invite-Code oder eine direkte Einladung beitreten.

1. Schauen Sie sich das Video „Didi erklärt Creative Commons“ an. Sie finden es auf www.pebbleonline.de in der Gruppe „Regeln der Mediennutzung“. Alternativ können Sie dem Link „Was ist CC?“ folgen, der sich ebenfalls in dieser Gruppe befindet. Nutzen sie gegebenenfalls die Suchfunktion auf der Seite, falls sie ein Medium nicht finden können.
2. Suchen Sie im Internet nach jeweils einem CC-lizenzierten Bild sowie einem Musikstück.
3. Fügen Sie die Medien als Links zu ihrer Mediensammlung auf PeBBLe hinzu. In der Linkbeschreibung nennen sie die Nutzungsbedingungen für das jeweilige Medium, so wie die CC-Lizenz sie vorgibt. In der Gruppe „Freie Medien Finden“ auf www.pebbleonline.de finden sie Webseiten, die Ihnen bei der Suche helfen können.
4. Teilen Sie die Links zu Ihren Fundstücken mit Ihrer Klasse in der gemeinsamen Gruppe auf PeBBLe.

Das Filmen fremder Menschen

Wenn Sie ein Video drehen und veröffentlichen möchten, auf dem andere Personen zu sehen sind, gilt es Folgendes zu beachten: Das Filmen von Personen auf öffentlichen Plätzen ist erlaubt, solange mehrere Personen auf dem Bild abgebildet sind und sie nur als Beiwerk neben einer Landschaft oder Örtlichkeit erscheinen. Auch Personen auf öffentlichen Veranstaltungen, Versammlungen, in öffentlichen Aufzügen und ähnlichen Vorgängen, dürfen gefilmt werden. (§ 23KUG). Sobald Sie eine bestimmte Person durch eine Nahaufnahme in den Hauptfokus der Aufnahme stellen, sollten Sie sich eine Einverständniserklärung dieser Person holen. Sobald Sie den öffentlichen Raum verlassen und auf Privatgelände filmen, brauchen Sie eine Drehgenehmigung des Besitzers/Eigentümers.

In dieser Lerneinheit haben Sie nun die wichtigsten rechtlichen Grundlagen im Umgang mit digitalen Medien kennen gelernt. Nun liegt es an Ihnen, dieses Wissen in der Praxis anzuwenden und zu vertiefen.

AB: Die 7 Grundregeln des Bundesdatenschutzgesetzes (BDSG)

Füllen Sie den folgenden Lückentext mit den in der Tabelle genannten Begriffen sinnvoll aus:

datenverarbeitende Stelle	berichtigt	Auskunft	Informationen
Strafe	Gelöscht	eine Rechtsvorschrift	nachweispflichtig
zu seiner Person	gesperrt	gesichert	der Betroffene
Geldbuße	Stellen		

1. Verbot mit Erlaubnisvorbehalt:

Die Verarbeitung und Nutzung von personenbezogenen Daten ist nur zulässig, wenn **der Betroffene** zustimmt oder **eine Rechtsvorschrift** sie gestattet.

2. Information des Betroffenen:

Der Betroffene soll grundsätzlich aufgrund von Anzeige- und Benachrichtigungspflichten bzw. Registereinsichtsrechten **Informationen** dazu erhalten, wer welche Arten von Daten über ihn verarbeitet.

3. Transparenz gegenüber den Betroffenen:

Dem Betroffenen ist auf Antrag **Auskunft** über die **zu seiner Person** gespeicherten Daten sowie über **Stellen**, an die Daten übermittelt werden, zu geben.

4. Korrekturpflichten der speichernden Stelle:

Unrichtige Daten müssen **berichtigt** werden; unzulässig gespeicherte, nicht mehr benötigte oder bestrittene Daten müssen **gesperrt** oder **gelöscht** werden.

5. Pflicht zur Datensicherung:

Die Daten müssen vor Missbrauch, Verlust etc. **gesichert** werden.

6. Kontrolle:

Hinsichtlich der Einhaltung dieser Ge-/Verbote ist die **Daten verarbeitende** Stelle externen und internen Kontrollinstanzen **nachweispflichtig**.

7. Sanktionen:

Verstöße gegen diese Ge-/Verbote können **Strafe, Geldbuße** und Betriebsstilllegung zur Folge haben.